IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

First Named Applicant: Lotspiech	Art Unit: 2132
Serial No.: 09/575,740	Examiner: Lanier
Filed: May 22, 2000	**AM9-98-028-US2**
For: **COINCIDENCE-FREE MEDIA KEY BLOCK FOR CONTENT PROTECTION FOR RECORDABLE MEDIA**	May 13, 2004 750 B STREET, Suite 3120 San Diego, CA 92101

APPEAL BRIEF

This appeal brief is submitted under 35 U.S.C. §134. This appeal is further to Appellant's Notice of Appeal filed herewith.

Table of Contents

(1) Real Party in Interest

The real party in interest is IBM Corp.

(2) Related Appeals/Interferences

No other appeals or interferences exist which relate to the present application or appeal.

(3) Status of Claims

Claims 1-6, 10, and 11 are pending and finally rejected.

(4) Status of Amendments

An amendment cancelling Claims 7-9 has been submitted and presumably will be entered for purposes of appeal.

(5) Summary of Invention

Using Claim 1 as an example, the invention is a method for complicating a coincidence attack in a system for protecting content on recordable media that includes providing a single media key (block 28, figure 3, page 7) and then transforming the media key using a position-specific function with each of a sequence of positions to render a sequence of position-dependent media keys (block 30, figure 3). The method then includes encrypting each position-dependent media key with a respective position-dependent device key, block 32.

On the other hand, Claim 2 recites a system for complicating a coincidence attack in a system for protecting content on recordable media 16, page 5, figure 1. The system of Claim 2 includes a media key block (MKB) which in turn includes plural encrypted entries, with each entry having a position in the MKB. Each entry is established at least in part by transforming a key number using a position number representing the position in the MKB of the respective key number.

Contrast Claims 1 and 2 with Claim 10, which recites a computer program device that has means for receiving a media key block (MKB) having plural positions, with each position having a number related thereto. The device of Claim 10 also has means for accessing a device key. The device key is associated with a position corresponding to one of the positions of the MKB, and the position associated with the device key is known to the decryption computer. Means are provided for decrypting the number at a position in the

MKB corresponding to the position associated with the device key to render a decrypted position-dependent media key. Also, means reverse transform the position-dependent media key with a number representing the position of the position-dependent media key in the MKB to render a media key.

(6) Issues

(a) Whether Claim 2 is unpatentable under 35 U.S.C. §112 as being indefinite.

(b) Whether Claim 1 is unpatentable under 35 U.S.C. §102 as being anticipated by Angelo, USPN 5,923,754.

(c) Whether Claims 2-6 are unpatentable under 35 U.S.C. §102 as being anticipated by Angelo, USPN 5,923,754.

(d) Whether Claims 10 and 11 are unpatentable under 35 U.S.C. §102 as being anticipated by Angelo, USPN 5,923,754.

(7) Grouping of Claims

The rejected claims are grouped as indicated above (Claim 1 alone, Claims 2-6 together, and Claims 10 and 11 together) owing to the different ways in which they characterize the invention and the different grounds and reasons for rejecting them used by the examiner. For instance, Claim 1 explicitly recites a position-dependent function, whereas the other claims do not explicitly recite this. Moreover, Claim 1 is drawn to a method whereas Claim 2 essentially is drawn to a medium that can be used with a method but which itself might not execute the method and, hence, which perforce has patentably different limitations than Claim 1.

Claims 10 and 11 are similar to Claim 1 but drawn from the decryption side, and while they might or might not implicitly require a salient feature of Claim 1 argued below (position-dependent function), they certainly do not explicitly contain such a recitation and, hence, should be considered separately from Claim 1. Perhaps more importantly, Claim 10 has not to date been specifically mentioned in any Office Action discussing Angelo. It would be simply improper to sustain a rejection of a claim that is not mentioned relative to a reference by lumping that claim in with other claims that have been treated.

(8a) Argument

Claim 2 has been rejected as being indefinite based on the allegation that when Appellant recites "***the*** position in the MKB of the respective key number", the definite article is improper because it allegedly lacks antecedent basis. This is simply wrong. In cases wherein it is implicit that an element can have only one of a characteristic or property, use of the definite article before first referring to the characteristic or property using the indefinite article is not defective, MPEP §2173.05(e) (citing Ex Parte Porter). Here, no showing has been made that a device key can have more than one position in a MKB; hence, use of the definite article to refer to "position" instead of the indefinite not only is proper (because it is not uncertain as to what is meant), but grammatically is preferable.

(8b) Argument

Claim 1 has been rejected under 35 U.S.C. §102 as being anticipated by Angelo based on the allegation that both the disk key of Angelo and a drive key derived from the disk key on power-up are position dependent, and similarly that combining the disk key and media key amounts to using a position

dependent function. The allegation is false, because the only way for it to be true is by pretending that certain claim limitations can be read so broadly as to effectively remove them from the claim.

Consider that Angelo's disk contains a single disk key (used in the rejection as the claimed "media key"). There is no position dependency of this key, other than being in some undisclosed location on a piece of media that itself can be located anywhere in the world. Angelo also has plural media keys, one for each piece of content on the disk. Upon power-up, the DVD player obtains the disk key from the disk and uses it to generate a drive key, which it uses to encrypt the product of the disk key and media key, for secure transmission of the keys to an associated video controller 18.

With this accurate summary of Angelo in mind, it is plain that the examiner strains too hard to arrive at a rejection when he conjures up position dependency in Angelo. There is none. For one thing, a key that is unique to a particular disk is not "position dependent", because the disk can be anywhere in the world and the key can be anywhere on the disk, and no matter what the location or position or orientation of the disk and/or key, the disk key remains the same. Second, the same is true of the relied-upon device key. The DVD player can be in any position/location/orientation and nothing about the device key is changed. Essentially, the examiner is reading position dependency out of the claims, because under his rationale any key anywhere is position dependent in that it is on some electronic media which is positioned somewhere in the world. This a particularly peculiar claim interpretation when one realizes that the words "location" and "position" are nowhere mentioned in Angelo in any context.

Third and specifically important to Claim 1, there is no position-dependent function in Angelo, because there is no concept of position dependency in Angelo. The alleged position-dependent function - the mere combination of the device key with the disk key/media key - does not depend on any position. It

depends on nothing more than combining two keys in a way that has nothing to do with a position, even if the keys themselves are (improperly) considered to be position dependent. The examiner disagrees but this disagreement is unreasonable. On the face of Angelo there is no position dependent function or key. Only the Red Queen in Alice in Wonderland, blessed as she is with the authority to redefine words as she see fit, can make such a claim, but unfortunately for the *prima facie* case there is no provision in the patent laws or regulations for recognizing her lexicography.

(8c) Argument

Apart from the above observations that Angelo fails to teach or suggest position dependent keys or functions, one other thing surely is in error, and that is the rejection of Claim 2, which requires not just any position dependency but explicitly requires that each entry in a media key block (MKB) is established by transforming a number using a position number representing the position in the MKB of the respective number. Plainly, even under the wildest interpretation of Angelo, no such thing remotely exists in it. There is no block, no key block, and no media block in Angelo. To date, nothing has been identified to the contrary apart from the frail and unsupported "finding" (based on no evidence of record) that for some reason Angelo's memory constitutes the claimed MKB, without the slightest acknowledgement that such a leap cannot legally be made unless prior art evidence is adduced that skilled artisans regard memories in general as being media key blocks. Otherwise, the claim term has been so broadly construed as to deprive it of any meaning and remove it from the claim altogether.

(8d) Argument

Claim 10 has also been rejected as being anticipated by Angelo, despite requiring a media key block (not taught in Angelo as shown above) that has plural positions with each position having a number related to it, despite requiring device keys that are associated with positions corresponding to one of the positions of the MKB (not taught in Angelo as shown above), and despite requiring decrypting the number at a position in the MKB corresponding to the position associated with the device key to render a decrypted position-dependent media key, which is not remotely approached by Angelo. With this in mind, the Examiner can be forgiven for his quite understandable reticence in explicitly acknowledging Claim 10 in the body of the discussion of Angelo, because it would require the continuing embarrassment of contending that a reference having no position dependence whatsoever in fact is rife with teachings of position dependency.

Respectfully submitted,

John L. Rogitz
Registration No. 33,549
Attorney of Record
750 B Street, Suite 3120
San Diego, CA 92101
Telephone: (619) 338-8075

JLR:jg

APPENDIX A - APPEALED CLAIMS

1. A method for complicating a coincidence attack in a system for protecting content on recordable media, comprising:

providing a single media key;

transforming the media key using a position-specific function with each of a sequence of positions to render a sequence of position-dependent media keys; and

encrypting each position-dependent media key with a respective position-dependent device key.

2. A system for complicating a coincidence attack in a system for protecting content on recordable media, comprising:

a media key block (MKB), the MKB including plural encrypted entries, each entry having a position in the MKB, each entry being established at least in part by transforming a key number using a position number representing the position in the MKB of the respective key number.

3. The system of Claim 2, wherein an entry is established by a media key.

4. The system of Claim 2, wherein each entry is established by the same media key as all other entries, the media key being combined with each of a sequence of positions to render a sequence of position-dependent media keys.

5. The system of Claim 4, wherein each position-dependent media key is encrypted by a respective device key.

6. The system of Claim 5, further comprising plural players, each having a device key of known position with which to decrypt the media key to play content encrypted with the media key.

10. A computer program device, comprising:

a computer program storage device including a program of instructions usable by a decryption computer, comprising:

logic means for receiving a media key block (MKB) having plural positions, each position having a number related thereto;

logic means for accessing a device key, the device key being associated with a position corresponding to one of the positions of the MKB, the position associated with the device key being known to the decryption computer;

logic means for decrypting the number at a position in the MKB corresponding to the position associated with the device key to render a decrypted position-dependent media key; and

logic means for reverse transforming the position-dependent media key with a number representing the position of the position-dependent media key in the MKB, to render a media key.

11. The computer program device of Claim 10, further comprising logic means for decrypting content using the media key.